UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/789,413	02/27/2004	Sandra E. Ring	2038	5254

7590 04/01/2008

Sandra E. Ring
9 Forest Street
Alexandria, VA 22305

EXAMINER	
REVAK, CHRISTOPHER A	
ART UNIT	PAPER NUMBER
2131	
MAIL DATE	DELIVERY MODE
04/01/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/789,413	RING ET AL.	
	Examiner	Art Unit	
	Christopher A. Revak	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 February 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,5-7,10,11,13,14 and 17-21* is/are rejected.

7)☒ Claim(s) *2-4,8,9,16 and 1215* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *27 February 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Specification

1. The disclosure is objected to because of the following informalities: On page 8 of the applicant's specification, line 21, reference is made to another co-pending application which the application number is missing.

Appropriate correction is required.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1,5-7,10,11,13,14, and 17-21 are rejected under 35 U.S.C. 102(e) as being anticipated by Flowers et al, U.S. Patent 7,073,198.

As per claim 1, it is taught by Flowers et al of a system for detecting an operating system exploitation which is of a type that renders a computer insecure, said system comprising a storage device; an output device; and a processor programmed to monitor the operating system to ascertain an occurrence of anomalous activity resulting from operating system behavior which deviates from any one of a set of pre-determined

operating system parameters, wherein each of said pre-determined operating system parameters corresponds to a dynamic characteristic associated with an unexploited said operating system; and generate output on said output device which is indicative of any said anomalous activity that is ascertained (col. 4, lines 38-61 and col. 6, lines 15-30 & 39-49).

As per claims 5,10, and 13, it is disclosed by Flowers et al wherein said exploitation is selected from a group of comprises consisting of a hidden kernel module, a hidden system call table patch, a hidden process, a hidden file and a hidden port listener (col. 4, lines 28-55).

As per claim 6, Flowers et al teaches of a system for detecting an operating system exploitation which is of a type that renders a computer insecure, said system comprising storage means; output means; processing means for monitoring the operating system to ascertain an occurrence of any anomalous activity resulting from behavior which deviates from any one of a set of pre-determined operating system parameters, wherein each of said pre-determined operating system parameters corresponds to a dynamic characteristic associated with an unexploited said operating system; and generating output on said output means which is indicative of any anomalous activity that is ascertained (col. 4, lines 38-61 and col. 6, lines 15-30 & 39-49).

As per claim 7, Flowers et al discloses of a computerized method for detecting exploitation of a computer operating system, comprising establishing a set of operating system parameters, each corresponding to a dynamic characteristic associated with an

unexploited operating system; monitoring the operating system to ascertain an occurrence of any anomalous activity resulting from behavior which deviates from any one of the set of operating system parameters; and generating output indicative of a detected exploitation upon ascertaining said anomalous activity (col. 4, lines 38-61 and col. 6, lines 15-30 & 39-49).

As per claim 11, it is taught by Flowers et al of a computerized method for detecting exploitation of a selected type of operating system, wherein the exploitation is one which renders a computer insecure, and whereby said method is capable of detecting said exploitation irrespective of whether the exploitation is signature-based and without a prior baseline view of the operating system, said method comprising monitoring the operating system to ascertain an occurrence of any anomalous activity resulting from behavior which deviates from any one of a set of operating system parameters, each operating system parameter corresponding to a dynamic characteristic associated with an unexploited operating system of the selected type (col. 4, lines 38-61 and col. 6, lines 15-30 & 39-49).

As per claim 14, it is disclosed by Flowers et al of a computer-readable medium for use in detecting rootkit installations on a computer running an operating system, said computer-readable medium comprising a loadable kernel module having executable instructions for performing a method comprising: monitoring the operating system to ascertain an occurrence of any anomalous activity resulting from behavior which deviates from any one of a set of dynamic operating system parameters, each operating system parameter corresponding to a dynamic characteristic associated with an

unexploited operating system of the selected type (col. 4, lines 38-61 and col. 6, lines 15-30 & 39-49).

As per claim 17, Flowers et al teaches of a computer-readable medium for use in detecting a rootkit exploitation of a computer running a Linux operating system, wherein said rootkit exploitation is of a type that renders the computer insecure, said computer-readable medium comprising a loadable kernel module having executable instructions for performing a method comprising analyzing the operating system's memory to detect an existence of any hidden kernel module; analyzing the operating system's system call table to detect an existence for any hidden patch thereto; analyzing the computer to detect an existence of any hidden process; and analyzing the computer to detect an existence of any hidden file (col. 4, lines 38-61 and col. 6, lines 15-30 & 39-49).

As per claim 18, Flowers et al discloses wherein said executable instructions are operative to analyze the computer for any hidden process by generating respective kernel space and user space views of running processes on the computer and ascertaining if a discrepancy exists therebetween (col. 4, lines 28-55).

As per claim 19, it is taught by Flowers et al wherein said executable instructions are operative to analyze the computer for any hidden file by generating respective kernel space and user space views of existing files on the computer and ascertaining if a discrepancy exists therebetween (col. 4, lines 28-55).

As per claim 20, it is disclosed by Flowers et al wherein said executable instructions are operative to analyze the system call table by initially obtaining an unbiased address for the system call table, and thereafter searching each call within the

system call table to ascertain if it references an address outside of a dynamic memory range for the operating system's kernel (col. 4, lines 28-55).

As per claim 21, Flowers et al teaches wherein said executable instructions are operative to display characteristic output results for any hidden kernel module, hidden system call table patch, hidden process and hidden file which is detected (col. 4, lines 28-55).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher A. Revak whose telephone number is 571-272-3794. The examiner can normally be reached on Monday-Friday, 9:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Christopher A. Revak/
Primary Examiner, Art Unit 2131